TRAFFIC AUTHENTICATION OF VERIFIED MEDIA PROGRAMMING PROVIDED OVER A COMPUTER NETWORK

Publication number:	WO03071737 (A1)
Publication date:	2003-08-28
Inventor(s):	HILL CLARKE RANDOLPH; STARR AARON D
Applicant(s):	MEASURECAST COM INC [US]
Classification:	
- international:	***G06F17/30; H04L9/32; H04L29/06; H04N5/00; H04N7/173;*** **G06F17/30; H04L9/32; H04L29/06; H04N5/00; H04N7/173;** (IPC1-7): H04L9/32; G06F17/30
- European:	H04L29/06C2; H04L29/06S12; H04N5/00N; H04N7/173B2
Application number:	WO2001US50035 20011231
Priority number(s):	WO2001US50035 20011231

Also published as:

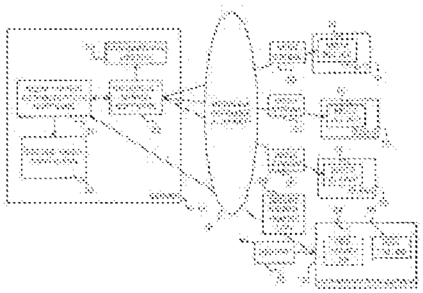
AU2002239686 (A1)

Cited documents:

US5956716 (A)
US6226618 (B1)
US2001051996 (A1)
US5450122 (A)
EP0817486 (A2)

Abstract of **WO 03071737 (A1)**

A media traffic authentication method provides authenticated information (30) about audio or video program (20) traffic over a computer network (16) from a media server (12). The method includes obtaining at the media server (12) a secure verification signature from the media segment (20) that is transmitted over a computer network (16) from the media server (12). The secure verification signature may include a digital watermark that is imperceptibly embedded in the media segment (20) or a checksum value that is calculated from the media segment (20), or a portion of it. A media traffic log (32) is generated at the media server (12) and includes information from the secure verification signature. In one implementation, the media traffic log (32) is secure (e.g., encrypted or digitally signed) with regard to the operator of the media server (12). The media traffic log (32) is transmitted to a media traffic authentication server (34) that is operated by a party other than the operator of the media server (12). A report (70) is then generated from the secure media traffic log (32) received at the media traffic authentication server summarizing media traffic at the media server (12).



Data supplied from the ***esp@cenet*** database — Worldwide

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 August 2003 (28.08.2003)

PCT

(10) International Publication Number
WO 03/071737 A1

(51) International Patent Classification[7]: H04L 9/32, G06F 17/30

(21) International Application Number: PCT/US01/50035

(22) International Filing Date: 31 December 2001 (31.12.2001)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: MEASURECAST.COM, INC. [US/US]; 921 SW Washington Steet, Suite 800, Portland, OR 97205 (US).

(72) Inventors: HILL, Clarke, Randolph; 921 SW Washington Street, Suite 800, Portland, OR 97205 (US). STARR, Aaron, D.; 921 SW Washington Street, Suite 800, Portland, OR 97205 (US).

(74) Agent: MEININGER, Mark, M.; Ipsolon LLP, 805 SW Broadway #2740, Portland, OR 97205 (US).

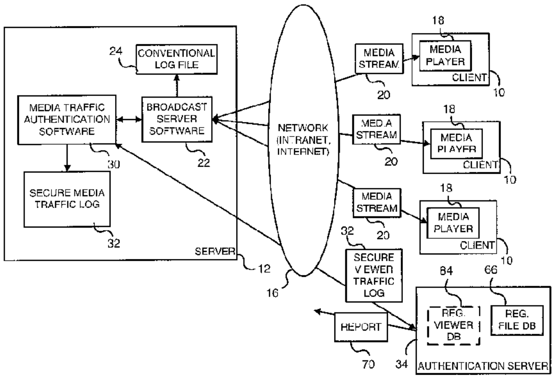
(81) Designated States *(national)*: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: TRAFFIC AUTHENTICATION OF VERIFIED MEDIA PROGRAMMING PROVIDED OVER A COMPUTER NETWORK



(57) Abstract: A media traffic authentication method provides authenticated information (30) about audio or video program (20) traffic over a computer network (16) from a media server (12). The method includes obtaining at the media server (12) a secure verification signature from the media segment (20) that is transmitted over a computer network (16) from the media server (12). The secure verification signature may include a digital watermark that is imperceptibly embedded in the media segment (20) or a checksum value that is calculated from the media segment (20), or a portion of it. A media traffic log (32) is generated at the media server (12) and includes information from the secure verification signature. In one implementation, the media traffic log (32) is secure (e.g., encrypted or digitally signed) with regard to the operator of the media server (12). The media traffic log (32) is transmitted to a media traffic authentication server (34) that is operated by a party other than the operator of the media server (12). A report (70) is then generated from the secure media traffic log (32) received at the media traffic authentication server summarizing media traffic at the media server (12).

WO 03/071737 A1

Traffic Authentication of Verified Media Programming Provided over a Computer Network

Field of the Invention

The present invention relates to measuring media traffic of audio or video programming delivered over a computer network and, in particular, to providing secure measurement of such media traffic.

Background and Summary of the Invention

In many countries, conventional broadcast radio and television programming are supported by advertising in the form of commercials that are interspersed throughout the programming. The costs for advertising during different radio and television shows depend upon sampled measurements of the numbers of people who listen to or watch those shows. (For purposes of simplicity, listeners and viewers are both referred to as viewers herein.) The most famous sampled measurements for programming are the Nielson ratings provided by Nielsen Media Research, Inc. and the Arbitron ratings provided by the Arbitron Company.

Transmission of audio and video programming over computer networks, such as the Internet, has become widely available and is becoming increasingly popular. Much of this online programming is being supported by advertising similar to the manner that advertising supports conventional broadcast programming. As with conventional broadcast programming, advertising costs are based upon measuring the numbers of users. As with conventional broadcast programming, measurement of numbers of viewers of online programming is typically conducted by sampled measurements and surveys.

Such sampled measurement of the viewers of online programming suffers from the disadvantage that many online broadcast programming sites might have insufficient traffic to be accurately measured by such sampling. Moreover, such sampling fails to utilize computer network transmission information that is commonly available in the form of network server log files.

A conventional log file typically includes a simple text listing of each file (e.g., media stream) that is transmitted by a media server to a client computer. A conventional log file typically will include information such as which media stream was transmitted (or requested), a network address (e.g., TCP/IP) identification of the client computer that requested (or to which was transmitted) the media stream, and the network browsing software and operating system of the client computer.

Typically, a conventional server log file is readily available to the operator of a server computer so that access to and usage of the server can be monitored. Numerous software utilities are available to provide summaries of usage information included in conventional server log files. Such usage information can be used by the operator of a server computer to discern usage patterns and correlate them with various business or marketing factors.

With advertiser support of a broadcast network site, both the advertisers and the operator of a server have direct economic interests in a conventional log file because advertising rates are typically tied directly to the sizes and types of viewer audiences (i.e., viewer traffic). However, the ready accessibility to and potential for improper manipulation of conventional log files by the operators of servers can render them an unreliable indication of viewer traffic from an advertiser's perspective. As a consequence, advertisers resort to sampled audience or traffic measurements by third parties to obtain objective measurements.

In contrast to the conventional sampled measurement of the sizes and types of viewer audiences, objective affirmation of the transmission of advertisements is commonly monitored directly. For example, conventional broadcasts may be monitored at any conventional receiver, and a log maintained by an observer who manually records which advertisements are transmitted. As another example, the monitoring of conventional broadcast advertisements at a receiver may be automated, as described by Adlink Information Network, Inc. of Pasig City, Phillipines, www.adlink.com.ph.

It will be appreciated, however, that such conventional receiver-based monitoring of advertisement transmission is ill-suited to transmission of programming over computer networks. Unlike conventional broadcasting, a single receiver location receiving programming over a computer network does not indicate that the programming is being widely distributed. The difference is that conventional broadcasting distributes programming to a universe of recipients (i.e., universal broadcasting), while programming is transmitted over a computer network to a particular recipient (i.e., individualized broadcasting). In view of this difference, conventional recipient monitoring of advertisement transmission is not suitable for programming that is transmitted over a computer network.

In accordance with the present invention, a media traffic authentication method provides authenticated server-side information about transmission of selected programming (e.g., advertisements) over a computer network from a media server. This method overcomes the limitations of conventional receiver-side monitoring of selected programming utilized for conventional or universal broadcasting.

In one implementation, the method includes obtaining at the media server a secure verification signature from a media stream (e.g., an advertisement or portion of it) that is transmitted over a computer network from the media server. The secure verification signature may include a digital watermark that is imperceptibly embedded in the media stream or a checksum value that is calculated from the media stream, or a portion of it. A media traffic log is generated at the media server and includes information from the secure verification signature. In one implementation, the media traffic log is secure (e.g., encrypted or digitally signed) with regard to the operator of the media server. The media traffic log is transmitted to a media traffic authentication server that is operated by a party other than the operator of the media server. A report is then generated from the secure media traffic log received at the media traffic authentication server summarizing media traffic at the media server. This provides objective server-side affirmation of the transmission of individualized programming (e.g., advertisements) over a computer network, together with the capability of measuring or identifying the audience to which the programming is broadcasted. In one implementation, the audience measurement and identification capabilities allow the objective affirmation of programming transmission to be applied to programming (e.g., advertisements) that is targeted to particular viewers or classes of viewers.

Additional objects and advantages of the present invention will be apparent from the detailed description of the preferred embodiment thereof, which proceeds with reference to the accompanying drawings.

Brief Description of the Drawings

Fig. 1 is a block diagram illustrating a computer network architecture as an operating environment for the present invention.

Fig. 2 is a flow diagram of a secure media traffic authentication method of the present invention.

Fig. 3 is a flow diagram of a viewer correlating method that may optionally be incorporated into the secure media traffic authentication method of Fig. 2.

Detailed Description of Preferred Embodiments

Fig. 1 is a block diagram illustrating a computer network architecture as an operating environment for the present invention. Multiple client computers or clients 10 are in communication with a server computer or server 12 via a network 16, such as a LAN, WAN, an intranet, or the Internet. Clients 10 and server 12 have, for example, conventional computer configurations that may include a high speed processing unit (CPU) in conjunction with a memory system (with volatile and/or non-volatile memory), an input device, and an output device, as is known in the art. Server 12 may be implemented as one or more server computers, which in the latter case may communicate with each other over one or more local or remote networks.

Each of clients 10 is a computer, such as a personal computer or computing device (e.g., handheld or embedded, such as network enabled stereo, television, car radio, etc.), running media player software 18 capable of playing or rendering graphic, audio or video files or portions of them (referred to as media segments 20). For example, media player software 18 may be Real Player™ from RealNetworks, Inc. of Seattle, Washington or Windows Media Player™ from Microsoft Corporation of Redmond, Washington. It will be appreciated that media player software 18 may be integral with or a plug-in added to commercially available network browser software, such as Netscape Navigator from Netscape Corporation or Internet Explorer from Microsoft Corporation, or may be an entirely separate application.

Server 12 is a computer with media broadcast server software 22 that provides serialized media, such as audio, video, or other media segments, to multiple client computers 10. For example, the serialized media may be in a streaming file format or in a serialized meta-file format in which an audio or video presentation may include multiple media segments. Examples of streaming file formats include RealMedia file formats promulgated by RealNetworks, Inc. An example of a serialized meta-file format is the SMIL (Synchronized Multimedia Integration Language) file format, which is sometimes referred to as a multimedia layout and integration language.

Server 12 is illustrated as being an originating server from which serialized media are transmitted. It will be appreciated, however, that server 12 could alternatively operate as a caching server or router that transmits serialized media received from another originating server. Accordingly, the present invention may be applied interchangeably or cumulatively to originating and caching servers.

Typically, a conventional log file 24 is generated by media broadcast server software 22 as it transmits media segments 20 to clients

10. Conventional log file 24 typically includes a simple text listing or record of each media segment 20 that is transmitted by broadcast server software 22. Typically, conventional log file 24 will have a format such as:

```
192.168.1.111 - - [21/Jul/2000:16:00:38 -0700]  "GET g2video.rm
RTSP/1.0" 200 261409 [WinNT_4.0_6.0.6.94_play32_RN6C_en-
US_686] [3f13ec98-2af0-11d4-9508-00b0d02359b1] [Stat1: 91 0 0
0 0 6_Kbps_Music][Stat2: 6000 15076 0 0 0 0 0 0 0 0 47
6_Kbps_Music] 1273163 59 14 0 0 1
```

and will include information such as which media segment 20 was transmitted (or requested), a network address (e.g., TCP/IP) identification of the client 10 that requested (or to which was transmitted) media segment 20, or its component, the network browsing software and operating system of client 10, etc.

Typically, conventional server log file 24 is readily available to the operator of server 12 so that access to and usage of server 12 can be monitored. Numerous software utilities are available to provide summaries of usage information included in conventional server logs 24. Such usage information can be used by the operator of a server computer to discern usage patterns and correlate them with various system diagnostics or business or marketing factors, as is known in the art.

With conventional computer network sites (sometimes called Web sites, in reference to the World Wide Web of the Internet), such usage information is often of primary economic interest to the operator of the server. In some instances of server 12 operating broadcast server software 22, the broadcasting of media segments 20 is supported by advertisers who pay the media broadcaster to transmit information such as advertisements with other media segments 20 that are directed to viewers. The broadcaster may be the operator of server 12 or may be a provider or owner of media segments 20 that is distinct from the operator of server 12, in which case the operator of server 12 may be a service provider for the broadcaster. For reference purposes, persons who listen to audio media or who view video media are referred to herein collectively and interchangeably as viewers. Advertiser payments to the broadcaster commonly relate to the numbers of viewers to whom media segments 20 are broadcast from server 12.

In these instances, both the advertisers and the operator of server 12 have direct economic interests in the information in conventional log file 24 because advertising rates and charges are typically tied directly to the sizes and types of viewer audiences (i.e., viewer traffic). However, the ready accessibility to and potential for improper manipulation of conventional log files 24 by the operator of server 12 can render log files 24 an unreliable indication of viewer traffic.

Accordingly, media server 12 includes server-side media traffic authentication software 30 that operates in conjunction with media broadcast server software 22. Media traffic authentication software 30 generates a secure media traffic log 32 that is distinct from conventional log 24 and is transmitted over network 16 to a viewer traffic authentication server 34, which typically would be operated by a party other than the operator of server 12. Viewer traffic authentication server 34 obtains viewer traffic information from secure viewer traffic logs 32 without risk of improper manipulation by the operator of server 12. The viewer traffic information from secure viewer traffic logs 32 may then be made available to advertisers and the operator of server 12 in a secure, impartial manner. Typically, traffic authentication server 34 would receive secure viewer traffic logs 32 from multiple broadcast servers 12 (only one shown).

In accordance with the present invention, media traffic authentication software 30 logs transmission of media segments 20 that have associated with them secure verification signatures. This allows media stream transmission verification that securely verifies transmission of media segments 20 that match or correspond to a predefined (e.g., registered) media segment master. The media segments 20 could correspond to particular content for which transmission is being paid, such as advertising content, or could correspond to other content. The media stream transmission verification provided by media traffic authentication software 30 generally includes identifying or finding a media segment 20 (e.g., an advertisment) in serialized media and verifying that the media segment 20 matches or corresponds to a pre-defined (e.g., registered) media segment master representing the authentic media segment to be transmitted.

In one implementation, identification of a media segment 20 and verification of a match between it and the pre-defined media segment master may be determined by a secure verification signature, such as a digital watermark, that is incorporated into the media stream 20. As is known in the art, digital watermarking, which is sometimes referred to as data embedding, is the process of imperceptibly embedding auxiliary data (e.g., text or a numeric ID) into a host audio, image, or video signal. The encoded signal generated by the data embedding process appears or sounds identical to the host signal. Products for providing digital watermarking are available from a number of companies, including Verance Corporation of San Diego, California, Cognicity, Inc. of Minneapolis, Minnesota, ALPHA-TEC LTD. of Greece, Digimarc Corporation of Tualatin, Oregon, etc.

In one implementation, media segment 20 may be identified upon detection of the digital watermark by the appropriate conventional digital watermark detection tool, whether hardware or software. In another implementation, media segment 20 may be identified by a meta-tag that is incorporated into media segment 20 to trigger reading of the digital watermark by the appropriate digital watermark detection tool. In either implementation, the digital watermark may include a secure identifier that correlates media segment 20 with its pre-defined media segment master.

Another implementation may employ hardware or software digital signal processing to calculate a fingerprint for a transmitted media segment 20, and then compare the digital signal processing fingerprint to one stored in a database for a pre-defined media segment master. Such digital signal process fingerprinting is described by, for example, Adlink Information Network, Inc. of Pasig City, Phillipines, www.adlink.com.ph, with reference to detecting conventional terrestrial broadcasting of advertisements.

In one implementation, the database of digital signal processing fingerprints may be local to server 12. In another implementation, the database of digital signal processing fingerprints may be maintained remotely from server 12, such as at the network site of a media transmission authentication service provider. In this implementation, the beginning and end of audio segments 20 could be identified by metadata included in the audio segments 20. The digital signal processing fingerprints for audio segments 20 could be stored in secure media traffic log 32 for later transmission to the network site of a media transmission authentication service provider for comparison with the stored digital signal processing fingerprints stored for the pre-defined media segment masters.

Despite the applicability of such digital signal process fingerprinting to the present invention, it will be appreciated that the detection of conventional terrestrial broadcasting of advertisements described by Adlink Information Network, Inc. provides merely confirmation of advertisement transmission, as received at a remote receiving station. The detection of conventional terrestrial broadcasting of advertisements described by Adlink Information Network, Inc. provides, therefore, no measure or identification of the actual recipients of the transmissions, as provided by the present invention.

In yet another implementation, the secure verification signature for a media segment 20 may be a checksum value that is associated with the media segment 20 according to a cyclic redundancy code (CRC), for example. As is known in the art, a checksum value for a selected computer file (e.g., a media segment 20) may be calculated with a predetermined algorithm, thereby creating a reference checksum value that uniquely corresponds to the selected media segment 20. As a result, later transmission of the selected media segment 20 can be verified by computing a checksum value for the file that is transmitted and comparing that checksum value with the reference checksum value. Generally, transmission of the selected computer file will result in a checksum value that matches the reference checksum value, and a different checksum value will result from transmission of a modification of the selected computer file or a file other than the selected computer file.

Many cyclic redundancy code algorithms for determining checksum values are directed to error detection applications and will provide different checksum values for any differences between original and subsequent computer files. For computer files that may be transmitted with different degrees of information resolution, as in many streaming media transmission applications, such highly accurate checksum value determinations may incorrectly indicate differences between a media segment 20 in its original form and a form corresponding to a lower resolution of the original. With regard to streaming media segment transmissions, therefore, checksum values are preferably determined by a cyclic redundancy code algorithm in which minor differences between files will result in matching checksum values, thereby accommodating data resolution differences in some streaming media applications.

Fig. 2 is a flow diagram of a secure media traffic authentication method 50 for media segments 20 having associated secure verification signatures. For purposes of illustration, traffic authentication method 50 is described as being performed by media traffic authentication software 30 and traffic authentication server 34. Traffic authentication method 50 represents one implementation of the operation of media traffic authentication software 30 and traffic authentication server 34 and the operation of them in other implementations may differ from traffic authentication method 50.

Process block 52 indicates that a media segment 20 is transmitted from a server computer, such as server 12.

Inquiry block 54 represents an inquiry as to whether the media segment 20 is identified as having associated with it a secure verification signature. For example, each media segment 20 having an associated secure verification signature may also include one or more identifying meta-tags. The identifying meta-tags may identify the media segment 20, or a portion of it, with which the secure verification signature is associated. In one implementation, the one or more meta-tags may include a START meta-tag indicating the beginning of media segment 20, or portion of it, and an END meta-tag indicating the end of media segment 20, or portion of it.

In addition, the one or more meta-tags may also include a FILE ID meta-tag that uniquely identifies the media segment 20 by, for example, a universally or globally unique identifier (GUID) or an identifying string such as "broadcaster.com/ads/foo.ad." If the media segment 20 is identified as having associated with it a secure verification signature, inquiry block 54 proceeds to process block 56. If the media segment 20 is not identified as having associated with it a secure verification signature, inquiry block 54 returns to process block 52.

Process block 56 indicates that a secure verification signature is obtained from the media segment 20. With the secure verification signature implemented as a digital watermark, for example, media traffic authentication software 30 may include a digital watermark reader software component that reads and decodes the digital watermark in the media segment 20. With the secure verification signature implemented as a checksum value, for example, media traffic authentication software 30 includes a checksum value calculator software component that computes a checksum value for the media segment 20.

Process block 60 indicates that secure media traffic log 32 is formed on broadcast server 12 to include information corresponding to secure verification signatures obtained from media segments 20. Secure media traffic log 32 is secure in that it is encrypted (e.g., public-private key encryption) or otherwise secured (e.g., digitally signed) to prevent log 32 from being modified or viewed by the operator of server 12, or to indicate if log 32 was modified by the operator of server 12. Secure media traffic log 32 may include information relating to secure verification signatures obtained from one or more media segment s 20.

With the secure verification signature implemented as a digital watermark, for example, secure media traffic log 32 may include for each broadcasted media segment 20 a media segment identifier that is obtained from the decode watermark and may include a globally unique identifier or another file identification indication. With the secure verification signature implemented as a checksum value, for example, secure media traffic log 32 may include for each broadcasted media segment 20 a checksum value that is calculated by the calculator software component for the media segment 20.

Process block 62 indicates that secure media traffic log 32 is transmitted over network 16 to media traffic authentication server 34. Secure media traffic log 32 may be transmitted to media traffic authentication server 34 separately for each information entry (i.e., for each media segment 20), or may be transmitted to media traffic authentication server 34 periodically, such as daily or more frequently (e.g., hourly), for batches of multiple information entries.

Process block 64 indicates that media segments 20 listed in secure media traffic log 32 are compared against a registered or master media segment database 66 that is stored on or in association with media traffic authentication server 34, thereby to authenticate the media streams 20 that are transmitted from server 12. With the secure verification signature implemented as a digital watermark, for example, the media segment identifier incorporated into the digital watermark is stored in registered or master media segment database 66 in association with other information about the media segment, such as its sponsor, creator, date of creation, etc. With the secure verification signature implemented as a checksum value, for example, the checksum value determined from the original media segment is stored in registered media file database 66 in association with other information about the media segment, such as its sponsor, creator, date of creation, etc.

Process block 68 indicates that a report 70 is generated summarizing the media traffic information, and any associated demographic information, relating to operation of a media server 12.

Process block 72 indicates that report 70 is provided or made available to subscribers to the media traffic authentication service, including the operator of server 12 and advertisers, or their representatives.

Fig. 3 is a flow diagram of a viewer correlating method 80 that may optionally be incorporated into secure media traffic authentication method 50 to identify viewers receiving media segments 20 having associated secure verification signatures.

Process block 82 indicates that a client user registers as a registered user, which may include providing personal information, including demographic information, and being assigned a unique registered viewer identifier (e.g., a globally unique identifier, or GUID) that is automatically associated with media player software 18 on a client 10 operated by the user. The personal information are stored in a registered viewer database 84, which is shown in dashed lines, that is stored on or in association with media traffic authentication server 34. For example, the operator of a media traffic authentication service according to the present invention could obtain demographic information from users who elect to provide such information, in association with media content network sites that are served by the media traffic authentication service, or otherwise.

Process block 86 indicates that client identifying information is obtained identifying a client to which media segment 20 is transmitted. The operation of process block 86 may be performed in conjunction with the operation of process block 52, for example. In one implementation, media player software 18 on client 10 provides to server 12 the registered viewer identifier, either alone or in addition to conventional network address (e.g., TCP/IP) information. Some implementations of media player software 18 are capable of providing to server 12 the GUIDs of clients 10 from which media segments 20 are requested.

Process block 88 indicates that the registered viewer identifier is stored in secure media traffic log 32 with the media segmentinformation corresponding to the secure verification signature obtained from media segments 20. The operation of process block 86 may be performed in conjunction with the operation of process block 60, for example. In one implementation, the clients 10 listed in secure media traffic log 32 would typically include registered viewers and unregistered viewers.

Process block 90 indicates that the secure media traffic log 32, with registered viewer identifier and associated media file information, is transmitted over network 16 to media traffic authentication server 34.

Process block 92 indicates that media segments 20 listed in secure media traffic log 32 are compared against a registered media file database 66 that is stored on or in association with media traffic authentication server 34, thereby to authenticate the media segments 20 that are transmitted from server 12.

Process block 94 indicates that the registered viewer identifier or identifiers listed in secure media traffic log 32 are compared against a registered viewer database 84, thereby to identify at least demographics of viewers to whom the media segments 20 are transmitted from server 12. As a result, report 70 generated in accordance with process block 68 may include demographic information about viewers to whom the authenticated media segments 20 are transmitted.

This allows the objective affirmation of programming transmission to be applied to programming (e.g., advertisements) that is targeted to particular viewers or classes of viewers. As is known, targeted advertisements may be sent to individual viewers based on their demographic characteristics so that different viewers of a program could receive different advertisements. The present invention provides objective and secure affirmation of the transmission of even targeted advertising, despite such programming typically being exceptionally difficult to monitor or measure.

Having described and illustrated the principles of our invention with reference to an illustrated embodiment, it will be recognized that the illustrated embodiment can be modified in arrangement and detail without departing from such principles. It should be understood that the programs, processes, or methods described herein are not related or limited to any particular type of computer apparatus, unless indicated otherwise. Various types of general purpose or specialized computer apparatus may be used with or perform operations in accordance with the teachings described herein. Elements of the illustrated embodiment shown in software may be implemented in hardware and vice versa.

In view of the many possible embodiments to which the principles of our invention may be applied, it should be recognized that the detailed embodiments are illustrative only and should not be taken as limiting the scope of our invention. Rather, we claim as our invention all such embodiments as may come within the scope and spirit of the following claims and equivalents thereto.

Claims

1. A computer-implemented media traffic authentication method for providing authenticated information about audio or video program traffic over a computer network from a media server, the method comprising:

obtaining at the media server a secure verification signature from a media segment transmitted over a computer network from the media server; and

generating at the media server a media traffic log that includes secure verification signature information relating to media segments transmitted or requested from the media server.

2. The method of claim 1 in which the secure verification signature includes a digital watermark that is incorporated into the media segment.

3. The method of claim 1 in which the secure verification signature includes a checksum value that is determined from the media segment.

4. The method of claim 1 further comprising:

transmitting the media traffic log to a traffic authentication server; and

correlating the secure verification signature in the media traffic log with a registered media segment database associated with traffic authentication server to authenticate the transmission of the media segment.

5. The method of claim 1 in which ones of the media segments are associated together in a serializing media file format.

6. The method of claim 5 in which the serializing media file format includes a streaming media file format.

7. The method of claim 1 in which in which the media traffic log includes traffic records listing segments transmitted to client computers and one or more of the client computers are identified by globally unique identifiers.

8. The method of claim 7 in which the traffic authentication server has associated with it a viewer demographics database that includes registered viewer demographic information and associated globally unique identifiers of client computers, the method further comprising correlating one or more of the client computers that are identified by globally unique identifiers with the registered viewer demographic information in the registered viewer database.

9. The method of claim 1 in which the media traffic log on the media server is secure with regard to the operator of the media server.

10. The method of claim 9 in which the secure media traffic log of media traffic information on the media server is encrypted.

11. The method of claim 9 in which the secure media traffic log of media traffic information on the media server is digitally signed.

12. In a computer-readable medium, media traffic authentication software for providing authenticated information about audio or video program traffic over a computer network from a media server, the method comprising:

software for obtaining at the media server a secure verification signature from a media segment transmitted over a computer network from the media server; and

software for generating at the media server a media traffic log that includes secure verification signature information relating to media segments transmitted or requested from the media server.

13. The medium of claim 12 in which the secure verification signature includes a digital watermark that is incorporated into the media segment.

14. The medium of claim 12 in which the secure verification signature includes a checksum value that is determined from the media segment.

15. The medium of claim 12 further comprising:

software for transmitting the media traffic log to a traffic authentication server; and software for correlating the secure verification signature in the media traffic log with a registered media segment database associated with traffic authentication server to authenticate the transmission of the media segment.

16. The medium of claim 12 in which ones of the media segments are associated together in a serializing media file format.

17. The medium of claim 16 in which the serializing media file format includes a streaming media file format.

18. The medium of claim 12 in which in which the media traffic log includes traffic records listing segments transmitted to client computers and one or more of the client computers are identified by globally unique identifiers.

19. The medium of claim 18 in which the traffic authentication server has associated with it a viewer demographics database that includes registered viewer demographic information and associated globally unique identifiers of client computers, the medium further comprising software for correlating one or more of the client computers that are identified by globally unique identifiers with the registered viewer demographic information in the registered viewer database.

20. The medium of claim 12 in which the media traffic log on the media server is secure with regard to the operator of the media server.

21. In a computer-readable medium, media traffic authentication software for providing authenticated information about serialized audio or video program traffic over a computer network from a media server, comprising:

software for generating on the media server a media traffic log of media traffic information relating to a secure verification signature of a serialized media segment that is transmitted or requested from the media server.

22. The medium of claim 21 in which the secure verification signature includes a digital watermark that is incorporated into the media segment.

23. The medium of claim 21 in which the secure verification signature includes a checksum value that is determined from the media segment.

24. The medium of claim 21 further comprising:

software for transmitting the media traffic log to a traffic authentication server; and

software for correlating the secure verification signature in the media traffic log with a registered media segment database associated with traffic authentication server to authenticate the transmission of the media segment.

25. The medium of claim 21 in which the serialized media segment includes a streaming media file format.

26. The medium of claim 21 in which in which the media traffic log includes traffic records listing segments transmitted to client computers and one or more of the client computers are identified by globally unique identifiers.

27. The medium of claim 26 in which the traffic authentication server has associated with it a viewer demographics database that includes registered viewer demographic information and associated globally unique identifiers of client computers, the medium further comprising software for correlating one or more of the client computers that are identified by globally unique identifiers with the registered viewer demographic information in the registered viewer database.

28. The medium of claim 21 in which the media traffic log on the media server is secure with regard to the operator of the media server.

Fig. 1

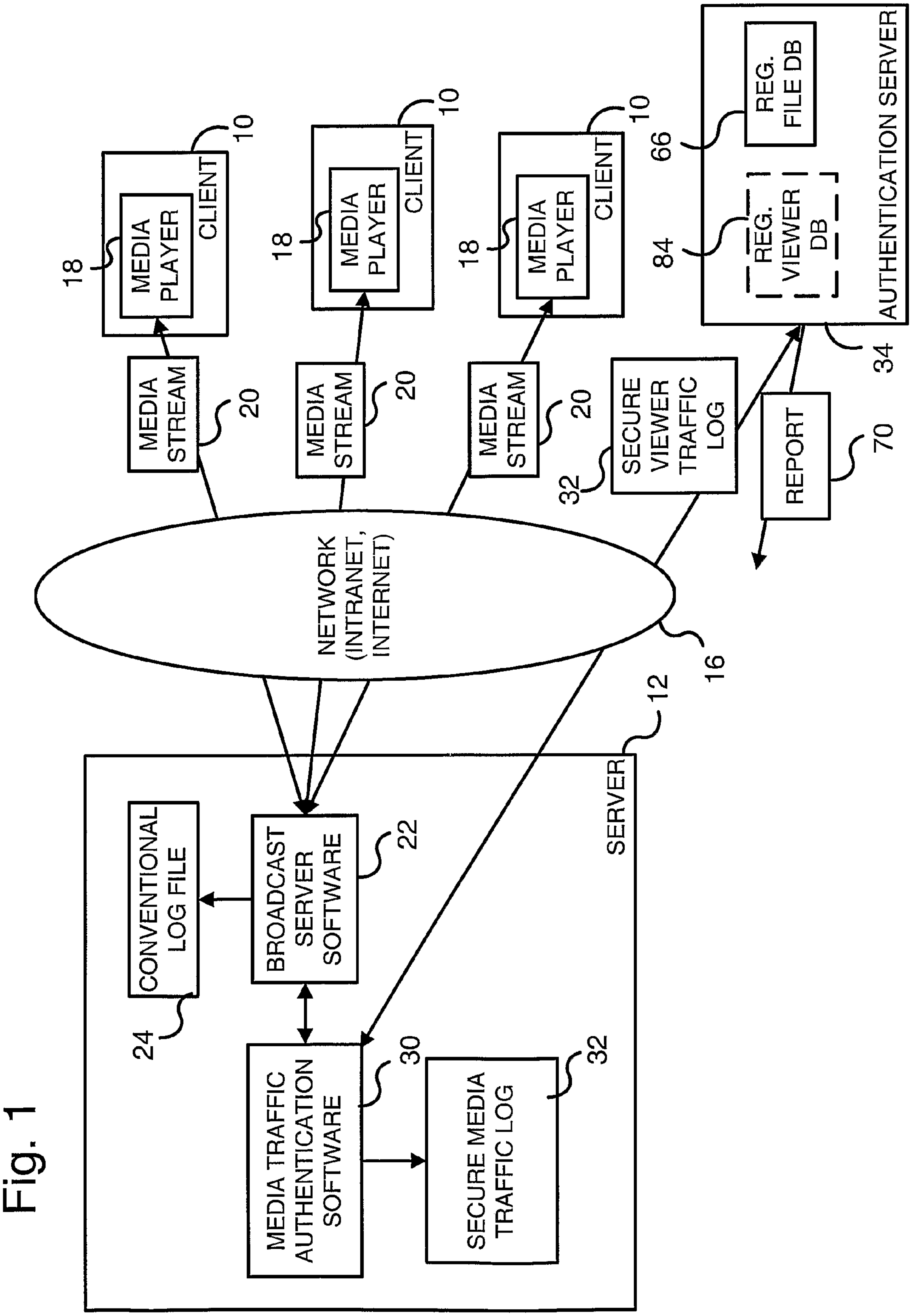

CLIENT
10
MEDIA PLAYER
18
MEDIA STREAM
20
REG. FILE DB
66
REG. VIEWER DB
84
AUTHENTICATION SERVER
34
SECURE VIEWER TRAFFIC LOG
32
REPORT
70
NETWORK (INTRANET, INTERNET)
16
SERVER
12
CONVENTIONAL LOG FILE
24
BROADCAST SERVER SOFTWARE
22
MEDIA TRAFFIC AUTHENTICATION SOFTWARE
30
SECURE MEDIA TRAFFIC LOG
32

Fig. 2

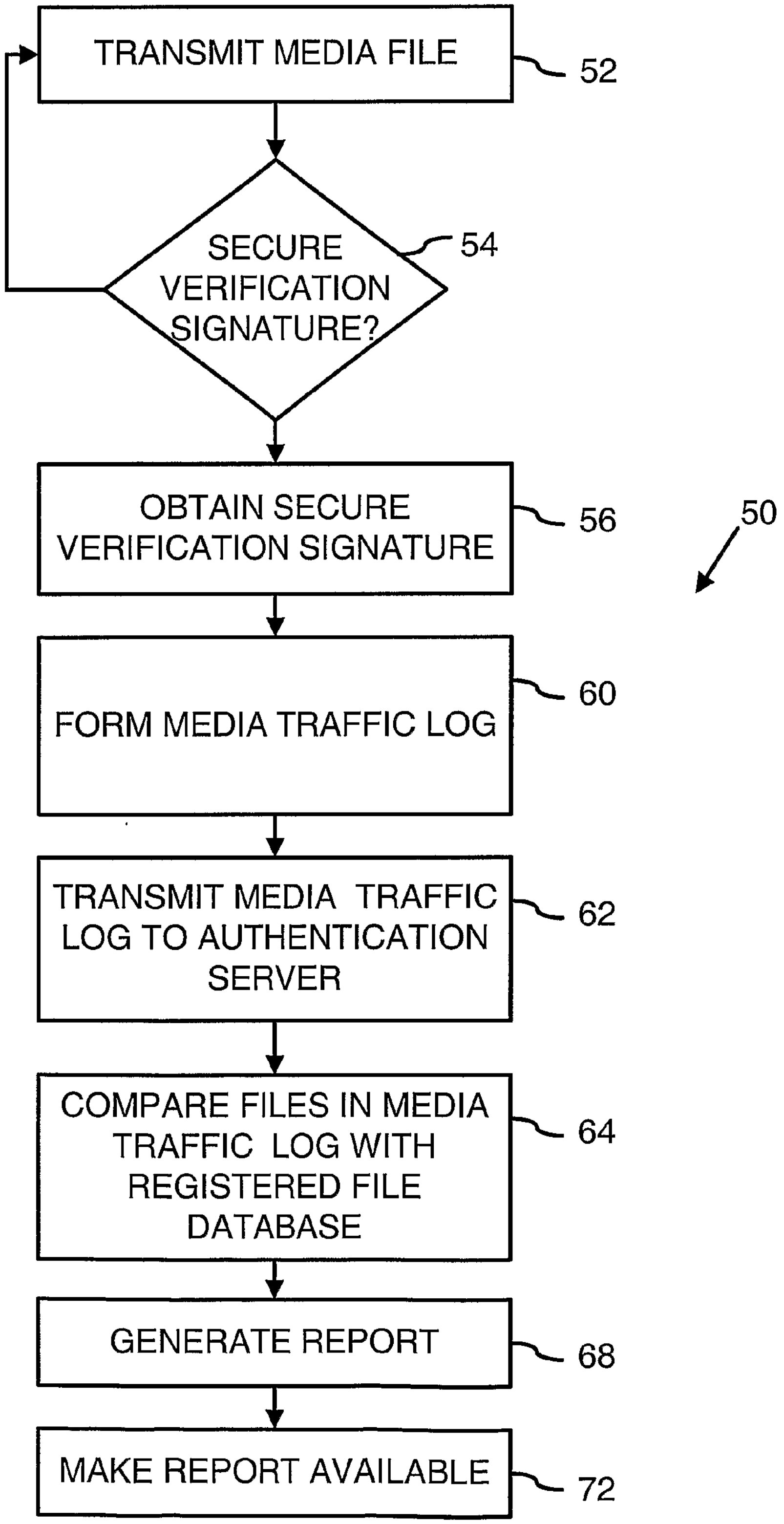
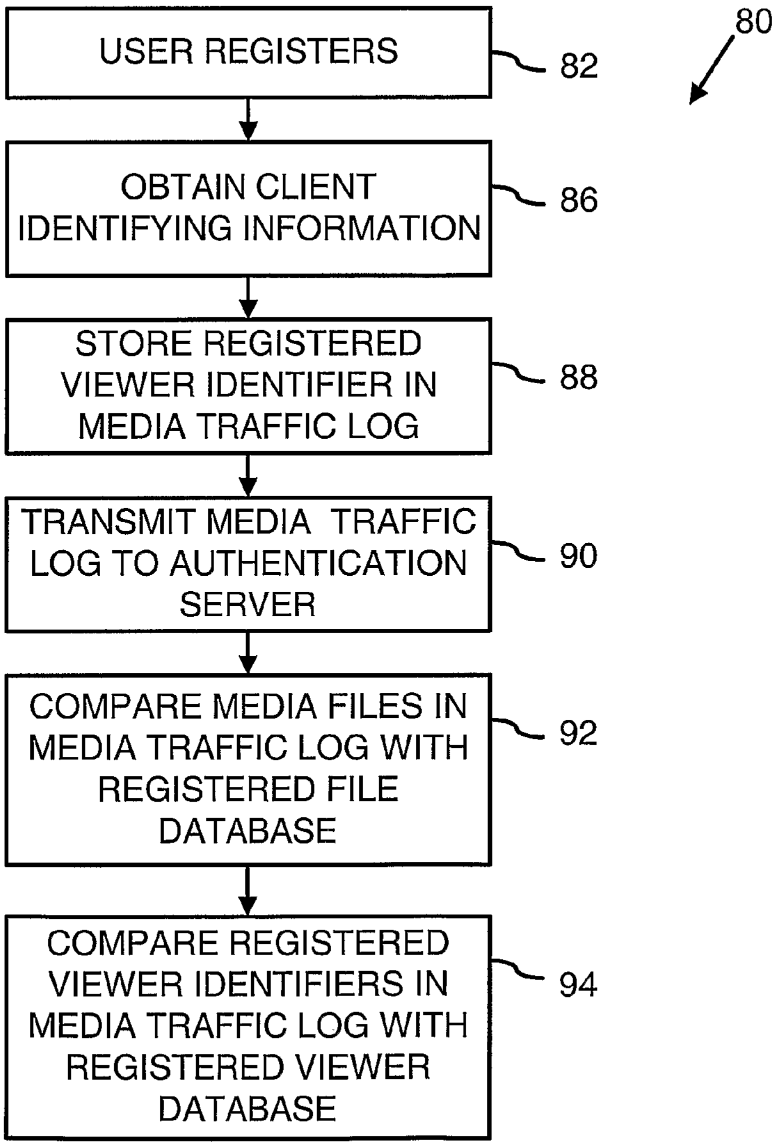

TRANSMIT MEDIA FILE
52
SECURE VERIFICATION SIGNATURE?
54
OBTAIN SECURE VERIFICATION SIGNATURE
56
50
FORM MEDIA TRAFFIC LOG
60
TRANSMIT MEDIA TRAFFIC LOG TO AUTHENTICATION SERVER
62
COMPARE FILES IN MEDIA TRAFFIC LOG WITH REGISTERED FILE DATABASE
64
GENERATE REPORT
68
MAKE REPORT AVAILABLE
72

Fig. 3


80
USER REGISTERS
82
OBTAIN CLIENT IDENTIFYING INFORMATION
86
STORE REGISTERED VIEWER IDENTIFIER IN MEDIA TRAFFIC LOG
88
TRANSMIT MEDIA TRAFFIC LOG TO AUTHENTICATION SERVER
90
COMPARE MEDIA FILES IN MEDIA TRAFFIC LOG WITH REGISTERED FILE DATABASE
92
COMPARE REGISTERED VIEWER IDENTIFIERS IN MEDIA TRAFFIC LOG WITH REGISTERED VIEWER DATABASE
94

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US01/50035

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 9/32; G06F 17/30
US CL : 713/176; 705/51
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : Please See Continuation Sheet

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 5,956,716 A (KENNER et al.) 21 September 1999 (21.09.1999), column 6, lines 41-52; column 7, Table 1, lines 51-56; column 8, lines 34-65; column 13, lines 9-34; column 21, lines 36-67; column 22, lines 1-47; and figure 1, item 18.	1, 4-8, 12, 15-19, 21, 24-27 ---------- 3, 14, 23
X --- Y	US 6,226,618 B1 (DOWNS et al.) 01 May 2001 (01.05.2001), column 11, lines 1-15; column 18, step 125; and figure 1C, item 105.	1, 2, 4, 7, 12, 13, 15, 18, 21, 22, 24, 26 ---------- 3, 14, 23
X --- Y	US 2001/0051996 A1 (COOPER et al.) 13 December 2001 (13.12.2001), page 5, paragraph [0058]; page 9, paragraph [0129] and [0134]; page 13, paragraphs [0199]-[0200]; figure 2, items 260 and 210; and figure 3, steps 320 and 350.	1, 2, 9-13, 20-22, 28 ---------- 2, 14, 23
Y	US 5,450,122 A (KEENE) 12 September 1995 (12.09.1995), column 15, lines 3-43; and figure 6, item 147.	3, 14, 23
A	EP 0 817 486 A2 (AT&T CORP.) 01 July 1998 (01.07.1998), column 8, lines 16-46; column 9, lines 29-40; and figure 5, steps 53, 54, and 57.	1, 4, 7, 8, 12, 15, 18, 19, 21, 24, 26, 27

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

02 August 2002 (02.08.2002)

Date of mailing of the international search report

05 SEP 2002

Name and mailing address of the ISA/US

Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703)305-3230

Authorized officer

Justin T. Darrow James R. Matthews

Telephone No. (703) 305-3900

INTERNATIONAL SEARCH REPORT

PCT/US01/50035

Continuation of B. FIELDS SEARCHED Item 1:
IPC(7) : H04L 9/32; G06F 15/16, 17/30, 17/60; H04N 7/16, 7/173

US CL : 713/162, 163, 176, 179, 182; 705/51, 56, 57, 58; 380/201, 202, 211, 212; 707/10, 100, 104; 709/217, 229

Continuation of B. FIELDS SEARCHED Item 3:
EAST (USPAT, EPO, JPO, DERWENT, US-PGPUB)
search terms: media, multimedia, medium, content, audio, video, program, transmit, distribute, broadcast, send, transfer, forward, download, receive, verify, identify, confirm, validate, authenticate, register, registry, database, directory, log, storage, memory, watermark, fingerprint, steganography, client, subscriber, user, customer, viewer, member.